SecureWave

2024 VULNERABILITY ASSESSMENT REPORT

June 2024

Prepared by
Luca Gaspari

Prepared for
Luca Gaspari

01

SecureWave

SecureWave S.r.l. è un'azienda leader nel settore della sicurezza informatica, specializzata nella protezione dei sistemi informatici e dei dati aziendali da minacce cyber. Con sede a Milano, Italia, SecureWave è stata fondata nel 2015 con l'obiettivo di fornire soluzioni di sicurezza informatica all'avanguardia a clienti di ogni settore.

La missione di SecureWave è proteggere le aziende dalle minacce informatiche, garantendo la sicurezza e l'integrità dei loro dati e sistemi. La visione dell'azienda è diventare il partner di fiducia per la sicurezza informatica a livello globale, offrendo soluzioni innovative e personalizzate per affrontare le sfide più complesse del settore.

Servizi Offerti

Vulnerability Assessment: SecureWave offre servizi di vulnerability assessment per identificare e valutare le vulnerabilità presenti nei sistemi informatici dei clienti. Questo servizio include una dettagliata analisi delle potenziali minacce e raccomandazioni per migliorare la sicurezza.

Penetration Testing: L'azienda esegue test di penetrazione simulando attacchi reali per scoprire punti deboli nei sistemi e fornire soluzioni per mitigare i rischi.

Managed Security Services: SecureWave fornisce servizi di gestione della sicurezza, monitorando continuamente le reti e i sistemi dei clienti per rilevare e rispondere a minacce in tempo reale.

Consulting e Compliance: L'azienda offre consulenza per la conformità normativa e l'implementazione di politiche di sicurezza, aiutando i clienti a rispettare le leggi e le normative vigenti in materia di protezione dei dati.

Formazione e Sensibilizzazione: SecureWave organizza corsi di formazione e programmi di sensibilizzazione per educare il personale aziendale sulle best practice di sicurezza informatica.

Contratto

Contratto di Servizio per Vulnerability Assessment e Penetration Test

Tra: Denim Solutions S.r.l.
Sede legale: Via Esempio, 123, 00100 Roma, Italia
P. IVA: 12345678901

E: SecureWave S.r.l.
Sede legale: Via Sicurezza, 45, 20100 Milano, Italia
P. IVA: 98765432109

Premesso che:

- Il Cliente desidera migliorare la sicurezza dei propri sistemi informatici.
- Il Fornitore è specializzato in servizi di sicurezza informatica, tra cui vulnerability assessment e penetration testing.
- Le parti hanno convenuto di eseguire i servizi con modalità white box, ovvero con piena conoscenza dei sistemi informatici da parte del Fornitore.

Si conviene e si stipula quanto segue:

Articolo 1: Oggetto del Contratto
Il Fornitore si impegna a fornire i seguenti servizi al Cliente:

1. Vulnerability Assessment: Analisi e valutazione delle vulnerabilità presenti nei sistemi informatici del Cliente.
2. Penetration Test: Simulazione di attacchi informatici per identificare e sfruttare potenziali vulnerabilità.

Articolo 2: Modalità di Esecuzione

1. White Box Testing: I test saranno eseguiti con piena conoscenza delle infrastrutture, delle architetture di rete, del codice sorgente e dei sistemi informatici del Cliente. Questo approccio consente un'analisi approfondita e accurata delle vulnerabilità.
2. Durata: I servizi saranno eseguiti nell'arco di 2 settimane, con un totale di 160 ore lavorative.

Articolo 3: Preventivo e Costi
Dettagli del Lavoro:

- Tariffa oraria: € 100/ora
- Durata stimata: 2 settimane (80 ore a settimana)
- Totale ore: 160 ore

Servizio	Ore	Tariffa Oraria (€)	Totale (€)
Vulnerability Assessment	80	100	8,000
Penetration Test	80	100	8,000
Totale Complessivo	160		**16,000**

Pagamenti:

- 50% all'inizio del progetto (€ 8,000)
- 50% alla consegna del rapporto finale (€ 8,000)

Articolo 4: Riservatezza

1. **Obblighi di Riservatezza:** Il Fornitore si impegna a mantenere riservate tutte le informazioni relative ai sistemi e ai dati del Cliente. Le informazioni ottenute durante l'esecuzione dei servizi saranno utilizzate esclusivamente per lo scopo del contratto.
2. **Durata della Riservatezza:** Gli obblighi di riservatezza rimarranno in vigore anche dopo la conclusione del contratto, per un periodo di 5 anni.

Articolo 5: Permessi e Accessi

1. **Accesso ai Sistemi:** Il Cliente fornirà al Fornitore tutti gli accessi necessari ai sistemi, alle reti e alle applicazioni per eseguire i test.
2. **Cooperazione:** Il Cliente coopererà pienamente con il Fornitore, fornendo tutte le informazioni e i documenti necessari per l'esecuzione dei servizi.

Articolo 6: Rapporti di Lavoro

Alla fine di ogni attività, il Fornitore consegnerà un rapporto dettagliato al Cliente contenente:

- Risultati del vulnerability assessment.
- Analisi dettagliata delle vulnerabilità trovate.
- Raccomandazioni e misure correttive.

Articolo 7: Responsabilità

Il Fornitore non sarà responsabile per eventuali danni diretti o indiretti derivanti dall'uso delle informazioni fornite. Il Cliente riconosce che l'esecuzione di penetration test può causare interruzioni o danni ai sistemi testati, e accetta tali rischi.

Articolo 8: Risoluzione del Contratto

Il contratto può essere risolto da entrambe le parti con un preavviso di 30 giorni. In caso di risoluzione anticipata, il Cliente sarà tenuto a pagare per i servizi effettivamente forniti fino alla data di risoluzione.

Articolo 9: Legge Applicabile e Foro Competente
Il presente contratto è regolato dalla legge italiana. Per qualsiasi controversia sarà competente il Foro di Milano.

Firmato:
Denim Solutions S.r.l.
Mario Rossi
SecureWave S.r.l.
Luca Gaspari

Contatti:
SecureWave S.r.l.
Via Sicurezza, 45, 20100 Milano, Italia
Telefono: +39 02 1234567
Email: info@securewave.it
Sito web: www.securewave.it

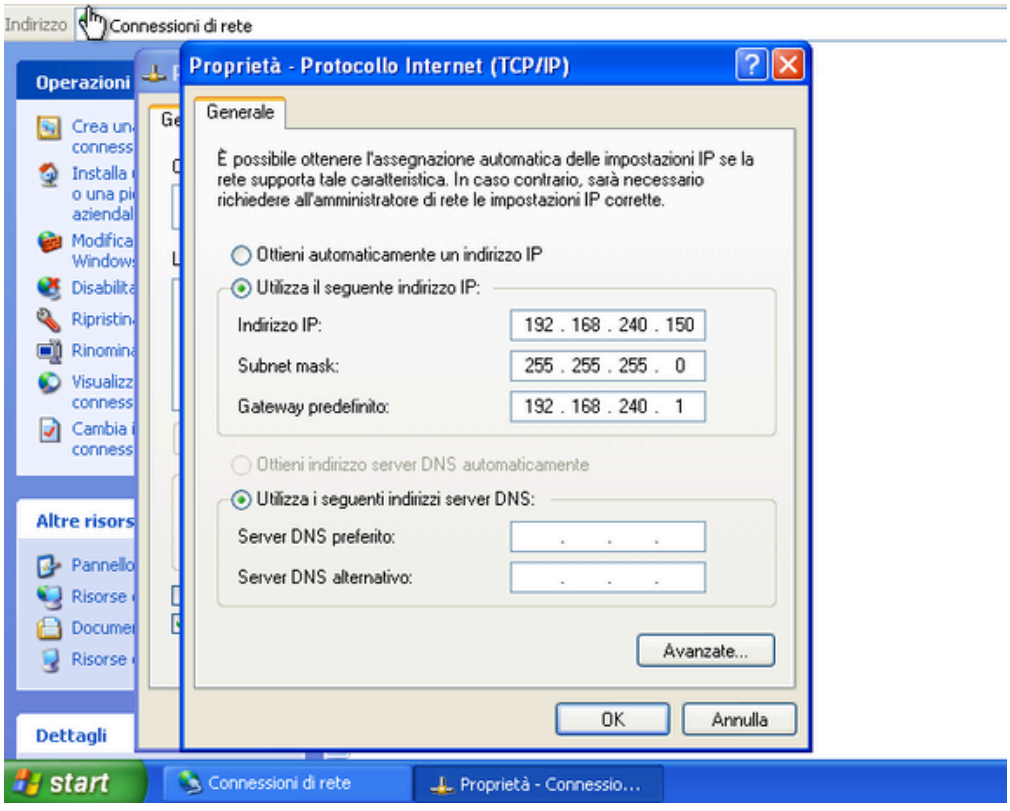
Introduzione

L'assessment è stato condotto su una macchina Windows XP (IP: 192.168.240.150) dalla nostra macchina Kali Linux (IP: 192.168.240.100). Sono stati effettuati vari test con il firewall della macchina Windows XP attivato e disattivato per analizzare le differenze nei risultati.

Configurazione della Rete

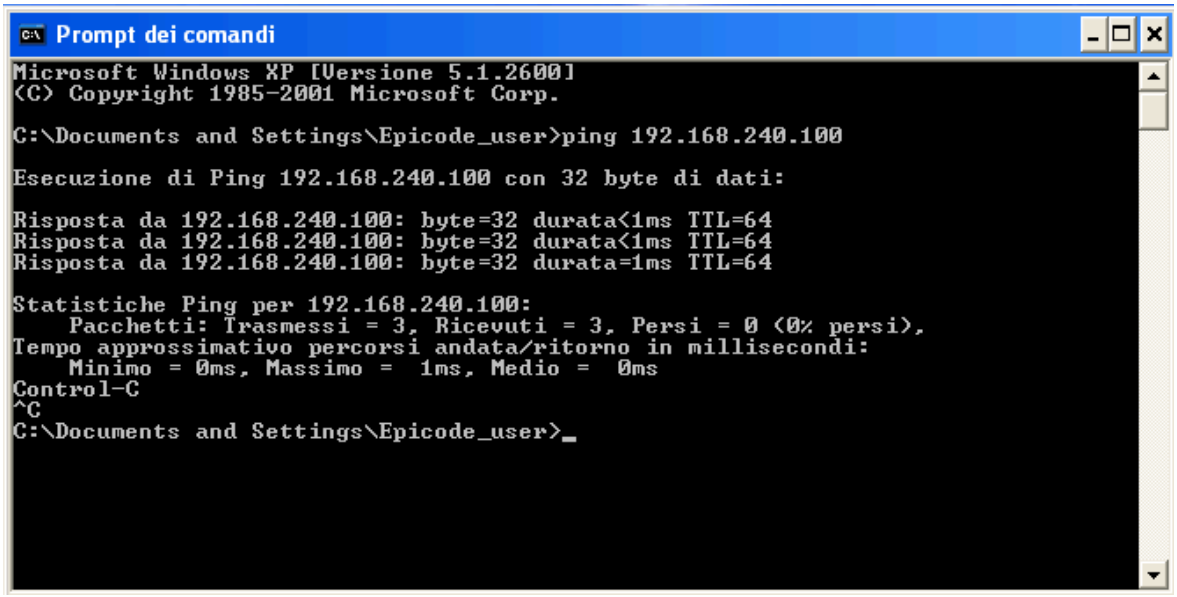
- Macchina Kali Linux: ip 192.168.240.100
- Macchina Windows XP: ip 192.168.240.150

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.240.100  netmask 255.255.255.0  broadcast 192.168.240.255
        inet6 fe80::a00:27ff:fe1e:364a  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:1e:36:4a  txqueuelen 1000  (Ethernet)
        RX packets 1  bytes 243 (243.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 16  bytes 2404 (2.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```



Ping tra le macchine

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.240.150
PING 192.168.240.150 (192.168.240.150) 56(84) bytes of data.
64 bytes from 192.168.240.150: icmp_seq=1 ttl=128 time=1.25 ms
64 bytes from 192.168.240.150: icmp_seq=2 ttl=128 time=1.59 ms
64 bytes from 192.168.240.150: icmp_seq=3 ttl=128 time=1.41 ms
64 bytes from 192.168.240.150: icmp_seq=4 ttl=128 time=0.349 ms
^C
── 192.168.240.150 ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 0.349/1.148/1.587/0.476 ms

┌──(kali㉿kali)-[~]
└─$
```



Scansione Nmap

Scansione senza firewall

Comando utilizzato: nmap -sV 192.168.240.150 -o esercizio1.txt

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.240.150 -o esercizio1.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 15:13 EDT
Nmap scan report for 192.168.240.150
Host is up (0.00043s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.55 seconds
```

Questo comando esegue una scansione di versioni dei servizi (-sV) sull'host con IP 192.168.240.150 e salva i risultati in un file chiamato esercizio1.txt. Con il firewall disattivato, Nmap è in grado di rilevare correttamente le porte aperte e i servizi in esecuzione sull'host.

Analisi:
Con il firewall disattivato, Nmap è stato in grado di rilevare correttamente l'host come attivo. Sono state trovate tre porte aperte con i rispettivi servizi:

- Porta 135/tcp: Servizio msrpc (Microsoft Windows RPC)
- Porta 139/tcp: Servizio netbios-ssn (Microsoft Windows netbios-ssn)
- Porta 445/tcp: Servizio microsoft-ds (Microsoft Windows XP microsoft-ds)

Questi risultati indicano che con il firewall disattivato, le porte aperte e i servizi esposti possono essere rilevati facilmente, evidenziando le potenziali vulnerabilità

Scansione con firewall attivo

Comando Utilizzato: nmap -sV 192.168.240.150 -o esercizio2.txt

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.240.150 -o esercizio2.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 15:16 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.17 seconds
```

Analisi:
Quando il firewall era attivo sulla macchina Windows XP, Nmap non è riuscito a rilevare l'host come attivo. Questo è dovuto al fatto che il firewall blocca le sonde di ping, facendo sembrare che l'host non risponda. Nmap suggerisce di utilizzare l'opzione -Pn per ignorare il ping e procedere comunque con la scansione delle porte.

Comando Utilizzato: nmap -Pn -sV 192.168.240.150 -o esercizio3.txt

```
┌──(kali㉿kali)-[~]
└─$ nmap -Pn -sV 192.168.240.150 -o esercizio3.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 15:18 EDT
Nmap scan report for 192.168.240.150
Host is up.
All 1000 scanned ports on 192.168.240.150 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 214.64 seconds
```

Analisi:
Utilizzando l'opzione -Pn, Nmap presume che l'host sia attivo anche se non risponde alle sonde di ping. Tuttavia, tutte le porte risultano filtrate, il che significa che il firewall sta bloccando l'accesso a tutte le porte TCP. Nmap non riesce a determinare quali servizi siano in esecuzione a causa delle restrizioni imposte dal firewall.

Differenze Riscontrate

- Con Firewall Attivo: Nmap non è stato in grado di rilevare l'host come attivo utilizzando le sonde di ping. Anche con l'opzione -Pn, tutte le porte risultavano filtrate, impedendo la rilevazione dei servizi.
- Con Firewall Disattivato: Nmap ha rilevato correttamente l'host e ha identificato tre porte aperte con i rispettivi servizi, indicando che l'host è molto più esposto senza le protezioni del firewall.

Conclusioni

- Firewall Attivo: Mantiene l'host nascosto dalle sonde di ping e blocca l'accesso a tutte le porte, aumentando significativamente la sicurezza.
- Firewall Disattivato: Espone l'host e i suoi servizi alle scansioni Nmap, rivelando potenziali punti di attacco.

Raccomandazioni

1. Mantenere il Firewall Attivo: È essenziale per proteggere l'host da accessi non autorizzati e scansioni potenzialmente dannose.
2. Aggiornamento e Patch: Applicare tutte le patch di sicurezza e aggiornamenti per mitigare le vulnerabilità note.
3. Limitare i Servizi Esposi: Rivedere e limitare i servizi in esecuzione sulla macchina per ridurre ulteriormente la superficie di attacco.
4. Monitoraggio Continuo: Implementare soluzioni di monitoraggio e logging per rilevare e rispondere tempestivamente a eventuali tentativi di intrusione.